10 August 2015

NORTH DAKOTA

HOMELAND SECURITY

Cyber Summary

The North Dakota Open Source Cyber Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Cyber Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Cyber Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

Table of Contents

North Dakota

Nothing Significant to Report

Regional

(South Dakota) Attorney: Dakota Dunes clinic cyber attack affects data for more than 13,000 patients. Siouxland Pain Clinic in Dakota Dunes notified over 13,000 patients July 31 that their personal and medical information may have been compromised in an attack on the clinic's server that occurred between March 26 and April 2. The clinic was notified of the breach June 26 and continues to investigate the incident.
http://siouxcityjournal.com/news/attorney-dakota-dunes-clinic-cyber-attack-affects-data-for-more/article_d1550c3e-3371-5701-802e-5c90a9b6a9a2.html

National

(National) New tool to improve government computer network security. Researchers have developed a computer network security tool to help government agencies, along with state and local governments. The software-based technology, known as the Network Mapping System (NeMS), discovers and characterizes computer networks. "It is important to know what you have on your networks, so that you can decide what best practices to apply," says one of the researchers.
http://www.homelandsecuritynewswire.com/dr20150806-new-tool-to-improve-government-computer-network-security

International

(International) Nuclear nightmare: Industrial control switches need fixing, now. Security researchers at Dragos Security discovered at least 11 vulnerabilities in control switches being used in industrial control systems (ICS) across multiple sectors that could allow an attacker to execute man-in-the-middle (MitM) attacks to cause control systems to shut down a plant or process or force an ICS into a hazardous state. Researchers believe that the attacks are being exploited in the wild, and that the vulnerabilities are made possible by poor authentication protocols and cryptographic integrity.

http://www.zdnet.com/article/nuclear-nightmare-industrial-control-switches-need-fixing-now/

(International) APT group gets selective about data it steals. Security researchers from the Dell SecureWorks Counter Threat Unit released findings from a report revealing that the Emissary Panda advanced persistent threat (APT) group has focused its efforts on a number of manufacturing, automotive, aerospace, pharmaceutical, oil and gas, defense industrial base, political, and education organizations in the U.S. and the United Kingdom, utilizing a number of tools to steal and transmit intellectual property via backdoors. https://threatpost.com/apt-group-gets-selective-about-data-it-steals/114103

(International) Russian government-backed hackers breach Joint Chiefs e-mail server. Russian government-backed hackers have managed to hack the Pentagon's unclassified e-mail server used by the office of the Joint Chiefs. Military officials said Thursday that the sophistication of the attack shows that it has been conducted by hackers with the resources typically available only to states. The e-mail system was taken offline as soon as the intrusion was detected. The required cyber protection measures and security patches were all in place, but the attackers still managed to circumvent them and find a way into the network in a manner that U.S. government cyber experts had not seen before, senior Defense officials said. http://www.homelandsecuritynewswire.com/dr20150807-russian-governmentbacked-hackers-breach-joint-chiefs-email-server

Banking and Finance Industry

Nothing Significant to Report

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

Nothing Significant to Report

Communications Sector

(International) Google patches DoS vulnerability affecting most Android Devices. Google informed Trend Micro of the availability of a fix on July 31. However, due to Android's fragmented ecosystem and the reliance on device manufacturers and carriers to push security updates, it will take some time until the patch reaches most users. Furthermore, the owners of older devices might never receive the patch.
http://www.securityweek.com/google-patches-dos-vulnerability-affecting-most-android-devices

(International) Your smartphone battery could be tracking you. The World Wide Web Consortium debuted the battery status API back in 2012 with the goal of helping websites maximize the battery life of mobile devices that visit them. The basic function allows websites to see how much battery life remains on any given device so the site can switch to a low-power mode if needed. The existing problem is that the W3C specification does not mandate user permission to query the device's battery life.
http://www.informationweek.com/mobile/mobile-devices/your-smartphone-battery-could-be-tracking-you/a/d-id/1321598

(International) Android device makers promise monthly security fixes. Google, Samsung, and LG announced plans to begin issuing monthly security patches for Android devices, citing the operating system's (OS) increased targeting from cybercriminals. The first large update includes a patch for the Stagefright vulnerability, which can compromise a device via a specially crafted multimedia message (MMS).
http://www.computerworld.com/article/2960512/security/android-device-makers-promise-monthly-security-fixes.html

(International) 80 vulnerabilities found in iOS in 2015, 10 in Android. Secunia released findings from a report on security vulnerability trends for the first 7 months of 2015 revealing an increase of "extremely critical" and "highly critical" threats, a trending increase in zero-day exploits, and a total of 80 reported vulnerabilities in Apple's iOS operating system (OS) versus 10 in Android devices. Researchers cited Apple's control of its OS and patch cycle as the cause for higher number if iOS vulnerabilities.

http://news.softpedia.com/news/80-vulnerabilities-found-in-ios-in-2015-10-in-android-488676.shtml

(International) **Easily exploitable Certifi-gate bug opens Android devices to hijacking.** Security researchers from Check Point's mobile security research team discovered a set of vulnerabilities in the Android operating system (OS) dubbed "Certifi-gate" in the architecture of mobile Remote Support Tools (mRSTs) used by almost every Android device manufacturer in which an attacker can leverage hash collisions, inter-process communication (IPC) abuse, and certificate forging to gain unrestricted device access and steal personal data, track locations, and turn on microphones, among other actions.
http://www.net-security.org/secworld.php?id=18730

Critical Manufacturing

(National) **Tesla Issues Fix After Researchers Hack a Model S and Bring It to a Stop.** Tesla Motors said on Thursday it has sent a software patch to address security flaws in the Model S sedan that could allow hackers to take control of the vehicle.
http://www.nbcnews.com/tech/security/tesla-issues-fix-after-researchers-hack-model-s-bring-it-n405251

(International) **Gone in less than a second.** A security researcher unveiled a wallet-sized device, called Rolljam, that can be hidden underneath a vehicle and can intercept codes used to unlock most cars and garage doors employing rolling codes, by jamming the signal and replaying the next rolling code in the sequence. The developer previously created a device that was able to intercept communication between certain vehicles and the OnStar RemoteLink mobile application to locate, unlock, and remotely start a vehicle.
Source: https://threatpost.com/gone-in-less-than-a-second/114154

Defense/ Industry Base Sector

(National) **Improving the security of data transfer.** Georgia Tech researchers were awarded $4.2 million from the Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory (AFRL) to improve how data is tracked between computers, Internet hosts, and browsers for better cyber security. The four-year project, titled "THEIA" after the Greek goddess of shining light, attempts

to shed light on exactly where data moves as it is routed from one Internet host to another and whether any malicious code, for example, is attached to data during transfer.
http://www.homelandsecuritynewswire.com/dr20150806-improving-the-security-of-data-transfer

Emergency Services

(Ohio) **Ohio prison yard free-for-all after drone drops drugs.** Ohio prisons have had incidents with drones hovering over their yards before. But the most recent one saw the unmanned aerial vehicle become a high-flying drug mule.
http://www.cnn.com/2015/08/04/us/prison-yard-drone-drugs-ohio/index.html\

Energy

(International) Trend Micro uncovers attacks on Internet-connected petrol stations. Trend Micro experts investigating data attacks against automated gas tank systems using a custom international honeypot dubbed GasPot presented research at Black Hat 2015 which found 12 pump identifications, 4 pump modifications and 2 denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks against the systems from February – July 2015. Researchers suspect that several hacktivist groups, including the Iranian Dark Coders Team and the Syrian Electronic Army, were behind the attacks, a majority of which targeted the U.S.
http://www.infosecurity-magazine.com/news/trend-micro-uncovers-attacks-on/

Food and Agriculture

Nothing Significant to Report

Government Sector (including Schools and Universities)

(International) Chinese VPN used by APT actors relies on hacked servers. Security researchers at RSA analyzed a Chinese virtual private network (VPN) service dubbed "Terracotta" and found that the service has at least 31 hacked Windows server nodes worldwide in hospitality, government organizations, universities, technology services providers, and private firms. Researchers have observed compromised servers running the Gh0st Remote Administration Tool (RAT), the Mitozhan trojan, and the Liudoor Backdoor, among others. http://www.securityweek.com/chinese-vpn-used-apt-actors-relies-hacked-servers

(National) **Labor Department vulnerable to data breach.** The inspector general's office released a report August 4 which found several cybersecurity gaps in the U.S. Department of Labor's information security program, including serious control deficiencies in how the department handles its personal identity verification (PIV) cards and related systems, as well as a lack of a system to lock out individuals after multiple unsuccessful log-in attempts, among other findings. The report stated that the department was made aware of the findings and continues to work to address the issues. http://www.washingtonexaminer.com/labor-department-vulnerable-to-data-breach/article/2569530

Information Technology and Telecommunications

(International) **Fake "Windows 10 Free Upgrade" emails deliver ransomware.** Security researchers from Cisco's Talos Group discovered a ransomware campaign in which attackers purporting to be from Microsoft send victims emails with a fake Windows 10 installer attached that is actually a variant of the CTB-Locker crypto-malware.
http://www.net-security.org/malware_news.php?id=3082

(International) **DNS server attacks being using BIND software flaw.** Security researchers from Sucuri reported that attackers have begun exploiting a denial-of-service (DoS) flaw in all versions of BIND 9 open-source Domain Name System (DNS) software that was patched the week of July 27. The company confirmed that two clients in different sectors had experienced attacks. http://www.computerworld.com/article/2955290/security/dns-server-attacks-begin-using-bind-software-flaw.html

(Canada) **Hover Resets User Passwords Due to Possible Breach.** Hover is a subsidiary of Canada-based Internet services and telecommunications company Tucows, one of the world's largest ICANN-accredited domain registrars. A hover representative states, "We did this as a precautionary measure because there

appears to have been a brief period of time when unauthorized access to one of our systems could have occurred.”
http://www.securityweek.com/hover-resets-user-passwords-due-possible-breach

(International) **RIG Exploit Kit 3.0 succeeded in infecting 1.25 million machines.** Trustwave researchers reported that version 3.0 of the RIG Exploit Kit (EK) infected an average of 27,000 machines a day, totaling 1.25 million infections, through various campaigns in which it predominantly leveraged Adobe Flash zero-day exploits exposed by a Hacking Team leak in July.
http://news.softpedia.com/news/rig-exploit-kit-3-0-succeeded-in-infecting-1-25-million-machines-488461.shtml

(International) **“Man-in-the-Cloud” attacks leverage storage services to steal data.** Findings from Imperva’s latest Hacker Intelligence Initiative report revealed that attackers can abuse popular cloud storage services for command and control (C&C) communications, endpoint hacking, remote access, and data exfiltration via Man-in-the-Cloud (MITC) techniques in which they access and decrypt stored user synchronization tokens.
http://www.securityweek.com/man-cloud-attacks-leverage-storage-services-steal-data

(International) **Design flaw in Intel processors opens door to rootkits, researcher says.** A security researcher from the Battelle Memorial Institute disclosed a vulnerability in the x86 processor architecture in which an attacker could install a rootkit in the processor’s System Management Mode (SMM), enabling destructive actions such as wiping the Unified Extensible Firmware Interface (UEFI) or re-infecting the operating system (OS) after a fresh install.
Source: http://www.networkworld.com/article/2965873/design-flaw-in-intel-processors-opens-door-to-rootkits-researcher-says.html#tk.rss_all

(International) **Updated DGA Changer malware generates fake domain stream.** Researchers from Seculert published findings from a report revealing that the DGA Changer downloader malware now has the capability to generate a stream of fake domains once it determines that it is being run in a virtual environment, the first reported instance of malware generating fake domain generation algorithms (DGA).

https://threatpost.com/updated-dga-changer-malware-generates-fake-domain-stream/114159

(International) **DDoS attacks rage on, primarily impacting U.S. and Chinese entities.** Kaspersky Lab released findings from its DDoS Intelligence Report Q2 2015, revealing that 77 percent of the distributed denial-of-service (DDoS) attacks from April to June impacted 10 countries, primarily the U.S. and China. The report recorded the longest attack at 205 hours, and the peak number at 1,960 May 7, attributing their popularity to the ease in which the attacks can be arranged. http://www.scmagazine.com/kaspersky-lab-releases-q2-ddos-report/article/431034/

(International) **BLEKey device breaks RFID physical access controls.** Researchers at Black Hat 2015 released details from a number of proof of concept attacks highlighting the weaknesses in the Wiegand protocol used in radio-frequency identification (RFID) readers and other proximity card devices, which they were able exploit by using a device dubbed BLEKey to read cleartext data sent from card readers to door controllers to clone cards or send data to a mobile application that can unlock doors remotely at any time. https://threatpost.com/blekey-device-breaks-rfid-physical-access-controls/114163

(International) **Attackers could use Internet route hijacking to get fraudulent HTTPS certificates.** Security researchers at Black Hat 2015 highlighted the threats posed by Border Gateway Protocol (BGP) hijacking attacks, also known as route leaking, in which an attacker could tailor attacks to specific geographic regions by tricking a certificate authority (CA) into issuing a valid certificate for a domain name that they do not own. http://www.computerworld.com/article/2959542/security/attackers-could-use-internet-route-hijacking-to-get-fraudulent-https-certificates.html#tk.rss_security

US-Cert Updates and Vulnerabilities

(International) **WordPress Releases Security Update.** WordPress released update 4.2.4. This release addresses six issues, including three cross-site vulnerabilities and a potential SQL injection. https://wordpress.org/news/2015/08/wordpress-4-2-4-security-and-maintenance-release/

(International) **Mozilla Releases Security Updates for Firefox and Firefox ESR.** The Mozilla Foundation has released security updates to address a critical vulnerability in the built-in PDF Viewer for Firefox and Firefox ESR. Exploitation of the vulnerability may allow an attacker to read and steal sensitive local files on the victim's computer.
https://www.us-cert.gov/ncas/current-activity/2015/08/06/Mozilla-Releases-Security-Updates-Firefox-and-Firefox-ESR

(International) **Sierra Wireless GX, ES, and LS gateways running ALEOS contains hard-coded credentials.** Sierra Wireless devices running ALEOS, including AirLink GX, ES, and LS gateways, contain multiple hard-coded accounts with root privileges. These accounts are enabled by default and accessible by telnet or SSH in systems using ALEOS 4.3.4 or earlier. The accounts also exist and are enabled in versions 4.3.5 to 4.4.1, though remote access is disabled by default.
http://www.kb.cert.org/vuls/id/628568

ICS-Cert Alerts & Advisories

Nothing Significant to Report

Public Health

(National) **Data of 4 million patients lost in MIE hacking.** The Indiana Attorney General announced that an estimated 1.5 million State residents and 3.9 million individuals from 11 healthcare providers and 44 radiology clinics nationwide may have been impacted by a May breach of Medical Informatics Engineering and its subsidiary NoMoreClipboard’s networks. Officials continue to investigate the attack, which allowed hackers to gain access to patients’ personal and medical information.
http://news.softpedia.com/news/data-of-4-million-patients-lost-in-mie-hacking-488319.shtml

(National) **FDA issues alert over vulnerable Hospira drug pumps.** Healthcare organizations were alerted by the U.S. Food and Drug Administration July 31 regarding cyber security risks associated with the use of Hospira Symbiq infusion systems following flaws discovered in 2014, which included security holes that can be remotely exploited by hackers in order to gain access to the devices and possibly change the dosage they deliver. The company has been working on developing a software update and the vendor is working to remove all of the infusion systems from the market until a permanent replacement is available. http://www.securityweek.com/fda-issues-alert-over-vulnerable-hospira-drug-pumps

Transportation

(International) American Airlines, Sabre said to be hit in hacks backed by China. American Airlines Group Inc., is investigating a suspected hack into its system after Sabre Corp., a clearinghouse for travel reservations which shares some network infrastructure with the airline, confirmed a recent breach possibly tied to the same China-linked hackers who targeted United Airlines, major American health insurers, and U.S. Government agencies. Sabre is unsure of the extent of the breach, but warns it may expose millions of flight records, hotel bookings, and car rentals. http://www.bloomberg.com/news/articles/2015-08-07/american-airlines-sabre-said-to-be-hit-in-hacks-backed-by-china

Water and Dams

Nothing Significant to Report

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165